

## MYSTERY MOUSE VIRUS FOUND IN PROSTATE CANCER PATIENTS

Researchers say they have found a virus in the prostate of some cancer patients—a remarkable discovery that may suggest micro-organisms could play a role in causing this cancer.

The virus, closely related to one previously found only in mice, was found in cancerous prostates removed from men with a certain genetic defect. The researchers, with the University of California, San Francisco, and the Cleveland Clinic, presented the findings at an American Society of Clinical Oncology meeting in San Francisco.

"We have made a very fascinating discovery never before seen in humans [of a virus] that is very similar to one found in a mammal that causes cancer," said Dr Eric Klein of the Cleveland Clinic. "But we have not proven this virus causes prostate cancer."

This finding has planted nagging suspicions in the minds of scientists that some diseases may play important roles alongside genetics, environment and chance in causing breast, stomach and several other forms of cancer.

Researchers are not sure how the mouse virus infected people, but suspect it has been passed on genetically for many generations.

"This is a class of virus no one would have looked for in prostate cancer," said



UCSF researcher Joe DeRisi, who developed the so-called "gene chip" that made the discovery. DeRisi's chip contains 20,000 snippets of vital genetic material from every known virus. It is the same chip that confirmed a previously undiscovered virus in the cold family that caused the SARS outbreak three years ago.

"We haven't really been thinking along those lines," said Dr Anthony Zietman, a radiation oncologist at Massachusetts General Hospital. "This is an interesting finding that will take off in a whole new direction."

(Source: San Jose Mercury News, 24 Feb 2006, <http://www.mercurynews.com/ml/mercurynews/living/health/13950601.htm>)

## HIGH-VOLTAGE ELECTRICITY DOSES KILL CANCER CELLS

Scientists from Old Dominion University and Eastern Virginia Medical School say they've killed melanomas in mice using extremely short, high-voltage doses of electricity. The researchers told the *Virginian-Pilot* that they've never had a tumour that did not respond to the treatment.

Richard Nuccitelli, associate professor of electrical and computer engineering at Old Dominion, said the method might eventually turn into an effective cancer treatment.

The electric bursts often disrupted the blood flow to the tumour cells and shrank their

nuclei by 50 per cent, Nuccitelli said. The tumours died after two or three weeks of treatments. Each session involved hundreds of electrical pulses, each less than one one-millionth of a second and carrying 4,000 volts.

Nuccitelli said he and his colleagues believe the process works by severely damaging DNA in the cells. The treatment produced no scarring and did not harm adjacent cells. All of the research mice survived, with no ill effects.

The scientists said additional research will be needed before they can experiment on people.

The research is to appear online in the journal *Biochemical and Biophysical Research Communications*.

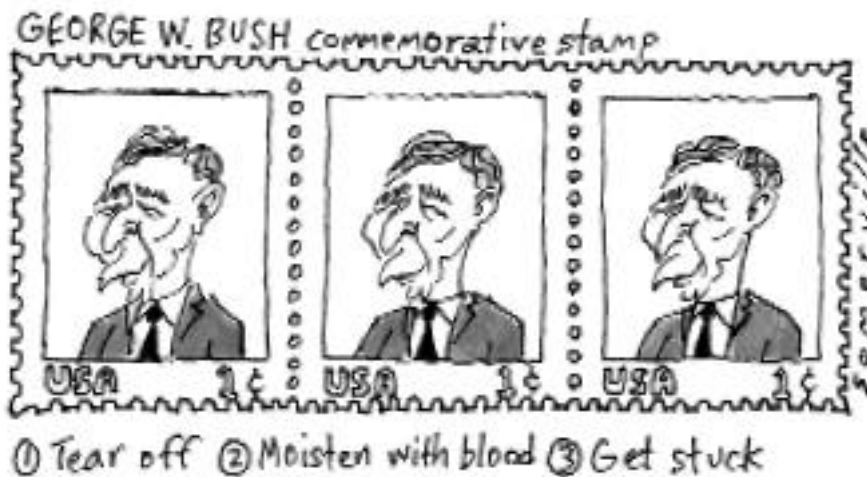
(Source: *Physorg.com*, 13 March 2006, <http://www.physorg.com/news11697.html>)

## BRAIN CELLS FUSED WITH SILICON CHIP

The line between living organisms and machines has just become a whole lot blurrier. European researchers have developed "neurochips" in which living brain cells and silicon circuits are coupled together.

The achievement will one day enable the creation of sophisticated neural prostheses to treat neurological disorders, or the development of organic computers that crunch numbers using living neurons.

To create the neurochip, researchers squeezed more than 16,000 transistors and hundreds of capacitors onto a silicon chip just one millimetre square in size.



They used special proteins found in the brain to glue brain cells—neurons—onto the chip. However, the proteins acted as more than just a simple adhesive.

"They also provided the link between ionic channels of the neurons and semiconductor material in a way that neural electrical signals could be passed to the silicon chip," said study team member Stefano Vassanelli from the University of Padua in Italy.

The proteins allowed the neurochip's electronic components and its living cells to communicate with each other. Electrical signals from neurons were recorded using the chip's transistors, while the chip's capacitors were used to stimulate the neurons.

"Pharmaceutical companies could use the chip to test the effect of drugs on neurons, to quickly discover promising avenues of research," Vassanelli said.

The researchers are now working on ways to avoid damaging the neurons during stimulation.

The team is also exploring the possibility of using a neuron's genetic instructions to control the neurochip.

(Source: *LiveScience*, 27 March 2006, [http://www.livescience.com/humanbiology/060327\\_neuro\\_chips.html](http://www.livescience.com/humanbiology/060327_neuro_chips.html))

## PHYSICISTS WARN AGAINST NUCLEAR WAR WITH IRAN

Thirteen of the most prominent physicists in the USA have written a letter to President Bush, calling US plans to reportedly use nuclear weapons against Iran "gravely irresponsible" and warning that such action would have "disastrous consequences for the security of the United States and the world".

The physicists include five Nobel laureates, a recipient of the National Medal of Science and three past presidents of the American Physical Society, the nation's pre-eminent professional society for physicists.

The letter was initiated by Jorge Hirsch, a professor of physics at the University of California, San Diego, who last autumn put together a petition signed by more than 1,800 physicists that repudiated new US nuclear weapons policies that include pre-emptive use of nuclear weapons against non-nuclear adversaries.

"The fact that the existence of this plan has not been denied by the Administration should be a cause of great alarm, even if it is only one of several plans being

considered," Professor Hirsch commented. "The public should join these eminent scientists in demanding that the Administration publicly renounce such a misbegotten option against a non-nuclear country like Iran."

The letter, which is available at web page <http://physics.ucsd.edu/petition/physicistsletter.html>, points out that "nuclear weapons are unique among weapons of mass destruction", and that in today's arsenals they have a total power of more than 200,000 times the explosive energy of the bomb that levelled Hiroshima, which caused the deaths of more than 100,000 people.

(Source: *University of California, San Diego*, 17 April 2006; *NewsWise*, <http://www.newswise.com/articles/view/519690/>)

## MI6 ADVERTISES FOR SPIES

A half-page advertisement in the *Times* careers supplement offers jobs for "operational officers", technology experts and "thoroughly efficient administrators".

MI6 has been shrouded in secrecy for most of its 97-year history. The organisation was not even officially acknowledged to exist until just over a decade ago.

"Staff who join SIS can look forward to a career that will have moments when the gap narrows just a little and the certainty of a stimulating and rewarding career which, like Bond's, will be in the service of their country," says the MI6 ad.

It says the agency operates around the world to make Britain "safer and more prosperous" and hires "people we can

depend on because everyone in the UK depends on them".

Those applying are warned that they should not tell anyone other than a spouse or closer partner that they are putting their name in.

(Source: *BBC News*, 27 April 2006)

## FORMER MI6 AGENT TOMLINSON STARTS BLOGSITE

Former MI6 agent Richard Tomlinson has decided to start his own blogsite in an effort to publicly air his long-running battle with his former employer.

Tomlinson was famously imprisoned in 1997 for breaking the 1989 Official Secrets Act by attempting to publish a book detailing his career. The book was finally published in 2001 after the Court of Appeal of England and Wales ruled in his favour.

It is alleged that Tomlinson published a list of 116 alleged MI6 agents on one of Lyndon LaRouche's websites. He has always denied being responsible for its publication. In the book, he states: "If MI6 had set out to produce a list that caused me the maximum incrimination, but caused them the minimum damage, they could not have done a better job." No definitive proof has ever been provided to link him with the list.

Says Tomlinson: "I've been involved in a long-running battle since April 25th, 1996, with my former employees, MI6 (British Secret Intelligence Service). ...MI6 relied on their considerable budget (from the taxpayer) and lots of threats, writs and pompous claims that I was a



'danger to national security', in order to silence and discredit me. They even managed to imprison me for a while.

"In order to keep me quiet and bash me around so much, they relied on the fact that a little guy like me did not have the financial means to fight back against their injunctions and legal assaults against me. But with a blog, I'm newly empowered—and how I wish I had known about them years ago..."

On the subject of MI6's recruitment campaign, Tomlinson says: "Good luck to any applicants: it is a very interesting career. I really enjoyed my time there. But be warned: they are a bullying employer, and are thoroughly vindictive towards any ex-employee who dares to criticise them.

"If I were to return to the UK, I would be arrested and imprisoned, simply for the crime of having written a book. It's not the sort of behaviour one would expect from a supposedly civilised employer in this day and age."

(Source: Richard Tomlinson blogsite, 9 April 2006, <http://www.richardtomlinson.typepad.com/>)

## DO DRUG COMPANY LINKS SWAY PSYCHIATRY?

A disturbing number of the experts who help write psychiatry's most influential diagnostic manual have financial ties to drug companies, raising concerns about the independence of diagnostic advice in the manual.

While such possible conflicts of interest are not uncommon, psychiatry is of

particular concern because diagnosis is so tricky. Physicians rely heavily on the *Diagnostic and Statistical Manual of Mental Disorders*, or *DSM*, which categorises psychiatric illnesses and their diagnostic criteria.

"The existence of disease categories validates the need for drugs," says Mildred Cho, a bioethicist at Stanford University in California. "Companies have an incentive to influence those creating the categories."

Lisa Cosgrove, a clinical psychologist at the University of Massachusetts in Boston, began to worry about such conflicts when she discovered that a majority of the members of a panel formed to consider whether to include "premenstrual dysphoric disorder" in the manual had received money from Eli Lilly. In 2000, Lilly won approval from the US Food and Drug Administration to market Prozac, rebranded as Sarafem, to treat the condition.

Together with Sheldon Krinsky of Tufts University in Medford, Massachusetts, Cosgrove looked at whether members of other *DSM* panels had financial ties to drug firms. Such ties included receipt of funding for research, acting as a consultant and being paid for speaking. Overall, 56 per cent of panel members had such links, and all members of the panels for "schizophrenia and other psychotic disorders" and "mood disorders" had such links (*Psychotherapy and Psychosomatics*, vol. 75, p. 154).

Even subtle changes to the *DSM* can have a big effect on patterns of prescribing.

This is a worry for conditions such as attention deficit hyperactivity disorder (ADHD).

"There has been a gradual broadening of the diagnostic criteria," says James Swanson of the University of California, Irvine.

Cosgrove and Krinsky found that 62 per cent of the *DSM* panel dealing with disorders such as ADHD had links to pharmaceutical firms.

The American Psychiatric Association (APA), which publishes the *DSM*, says its experts are not influenced by their financial ties. However, those recruited for the next edition, to appear in 2011, will be required to declare such interests.

Krinsky argues that the APA should ensure that no *DSM* panel has a majority of members with ties to drug companies. "It is time that the profession of psychiatry takes a serious look at itself from an ethical standpoint," he says.

(Source: by Peter Aldhous, *New Scientist*, 29 April 2006, <http://www.newscientist.com/article/mg19025494.100.html>)

## MERGER MAY CREATE AMERICA'S NEW SECRET POLICE

Intelligence experts warn that a proposal to merge two Pentagon intelligence units could create an ominous new agency. The turf grab by a controversial Pentagon intelligence unit is causing concern among both privacy experts and some of the Defense Department's own personnel.

An informal panel of senior Pentagon officials has been holding a series of unannounced private meetings during the past several weeks about how to proceed with a merger between the Counterintelligence Field Activity (CIFA), a post-9/11 Pentagon creation that has been accused of domestic spying, and the Defense Security Service (DSS), a well-established older agency responsible for inspecting the security arrangements of defence contractors. DSS also maintains millions of confidential files containing the results of background investigations on defence contractors' employees.

CIFA, a mysterious and secretive unit created in 2002, became the subject of public controversy when, late in 2005, documents surfaced indicating that CIFA had put together a database that included reports on anti-administration demonstrators including peace activists protesting alleged "war profiteering".

Both Pentagon insiders and privacy



"Why, yes, I am the CEO of a transnational oil company. How did you know?"

experts fear that if CIFA merges with, or, in effect, takes over DSS, there would be a weakening of the safeguards that are supposed to regulate the release of the estimated 4.5 million security files on defence-contractor employees currently controlled by DSS. Those files are stored in a disused mine in western Pennsylvania.

Defence analyst and *Washington Post* blogger Bill Arkin, who first brought allegations about CIFA's domestic spying to light, says that in trying to eliminate waste and better coordinate intelligence activities, "we are creating an American military secret police that is clearly acquiring way too much information and way too much power".

(Source: *Newsweek*, 14 April 2006, <http://www.msnbc.msn.com/id/12290187/site/newsweek/>)

## OLD SHIPS' LOGBOOKS UNLOCK EARTH'S MYSTERIES

The Earth's magnetic field has weakened by five per cent each century since 1840, when the first accurate measurements were made. But a new study looking at the magnetic field strength between 1590 and 1840 finds the field was relatively stable during that time.

The modelling of historical magnetic data was started in the early 1980s by study team member David Gubbins, a researcher from the University of Leeds, UK. The researchers began with readily available data like those in the logbooks of famed English sailor and explorer, James Cook.

Gubbins told *LiveScience* that they then "progressed to searching archives in Europe" and also found "50,000 'lost' 18th-century measurements in the East India Company archives in London".

Using the old sailing ships' logbooks, which recorded magnetic field directions useful in reconstructing field strength, and combining these records with a global model of directions, they produced 250 years' worth of measurement data.

This recent finding suggests that the current decline in field strength comes from growing and migrating patches of reverse magnetic flux in the southern hemisphere. The Earth's magnetic field has reversed many times.

The findings of this study are detailed in the 12 May 2006 issue of the journal *Science*.

(Source: *LiveScience*, 11 May 2006, [http://www.livescience.com/forcesofnature/060511\\_magnetic\\_logs.html](http://www.livescience.com/forcesofnature/060511_magnetic_logs.html))

## RFID CHIPS FALL PREY TO EASY HACKING

They can steal your smart card, lift your passport, jack your car, even clone the chip in your arm. And you won't feel a thing.

RFID chips are everywhere: companies and labs use them in access keys, Prius owners use them to start their cars, and retail giants like Wal-Mart have deployed them as inventory tracking devices. Drug manufacturers like Pfizer rely on chips to track pharmaceuticals. The tags are also about to get a lot more personal: next-generation US passports and credit cards will contain RFIDs, and the medical industry is exploring the use of implantable chips to manage patients.

According to the RFID market analysis firm IDTechEx, the push for digital inventory tracking and personal ID systems will expand the current annual market for RFIDs from US\$2.7 billion to as much as \$26 billion by 2016.

Dozens of companies, from Motorola to Philips to Texas Instruments, manufacture the chips. The tags work by broadcasting a few bits of information to specialised electronic readers. Most commercial RFID chips are passive emitters, which means they have no onboard battery; they send a signal only when a reader powers them with a squirt of electrons. Once juiced, these chips broadcast their signal indiscriminately within a certain range, usually a few inches to a few feet. Active emitter chips with internal power can send signals hundreds of feet; these are used in the automatic toll-paying devices that sit on car dashboards, pinging tollgates as autos whiz through.

For protection, RFID signals can be encrypted. The chips that will go into passports, for example, will likely be coded to make it difficult for unauthorised readers to retrieve their onboard information (which will include a person's name, age, nationality and photo). But most commercial RFID tags don't include security, which is expensive. This leaves most RFIDs vulnerable to cloning or—if the chip has a writable memory area, as many do—data tampering. Chips that track product shipments or expensive equipment, for example, often contain pricing and item information. These writable areas can be locked, but often they aren't because the companies using RFIDs don't know how the chips work or because the data fields need to be updated frequently. Either way, these chips are open to hacking.

"The world of RFID is like the Internet in its early stages," says Ari Juels, research manager at the high-tech security firm RSA Labs. "Nobody thought about building security features into the Internet in advance, and now we're paying for it in viruses and other attacks. We're likely to see the same thing with RFIDs."

Take the Future Store. Located in Rheinberg, Germany, the Future Store is the world's pre-eminent test bed of RFID-based retail shopping. All the items in this high-tech supermarket have RFID price tags, which allow the store and individual product manufacturers—Gillette, Kraft, Procter & Gamble—to gather instant feedback on what's being bought. Meanwhile, shoppers can check out with a single flash of a reader. In July 2004, *Wired* hailed the store as the "supermarket of the future". A few months later, German security expert Lukas Grunwald hacked the chips.

Grunwald co-wrote a program called RFDump, which let him access and alter price chips using a PDA (with an RFID reader) and a PC card antenna. With the store's permission, he and his colleagues strolled the aisles, downloading information from hundreds of sensors. They then showed how easily they could upload one chip's data onto another. "I could download the price of a cheap wine into RFDump," Grunwald says, "then cut and paste it onto the tag of an expensive bottle."

Today, Grunwald continues to pull even more elaborate pranks with chips from the Future Store. "I was at a hotel that used smart cards, so I copied one and put the data into my computer," Grunwald says. "Then I used RFDump to upload the room key card data to the price chip on a box of cream cheese from the Future Store. And I opened my hotel room with the cream cheese!"

In 1997, ExxonMobil equipped thousands of service stations with SpeedPass, which lets customers wave a small RFID device attached to a key chain in front of a pump to pay for gas. Seven years later, three graduate students, using a laptop and a simple RFID broadcasting device, tricked the system into letting them fill up for free from a gas station in Baltimore.

(Source: *Wired*, 6 May 2006, [http://www.wired.com/wired/archive/14.05/rfid\\_pr.html](http://www.wired.com/wired/archive/14.05/rfid_pr.html))